

Driving The Evolution of Trusted, Connected Computing

Lee Hirsch
Intel Corporation
January 20, 2000

Agenda

- What is “Trust”?
- Designing Security into the Computing Environment
- Privacy Considerations
- Policy Directions

Intel's Vision: A Trusted Connected World

- Secure Virtual Enterprises
 - “I can trust the Network with my business”
- Trillions of *Trusted* Transactions
 - “I can buy, trade, or sell anything on the Net”
- Ubiquitous Digital Content
 - “I can watch first-run movies over the internet”

Secure the Network, Platforms and Content

Top Security Concerns

Consumer:

- Malicious Code / Virus
- Privacy & Confidentiality
- Anonymity
- Ease of Use
- Know who you are dealing with on the Internet

Business:

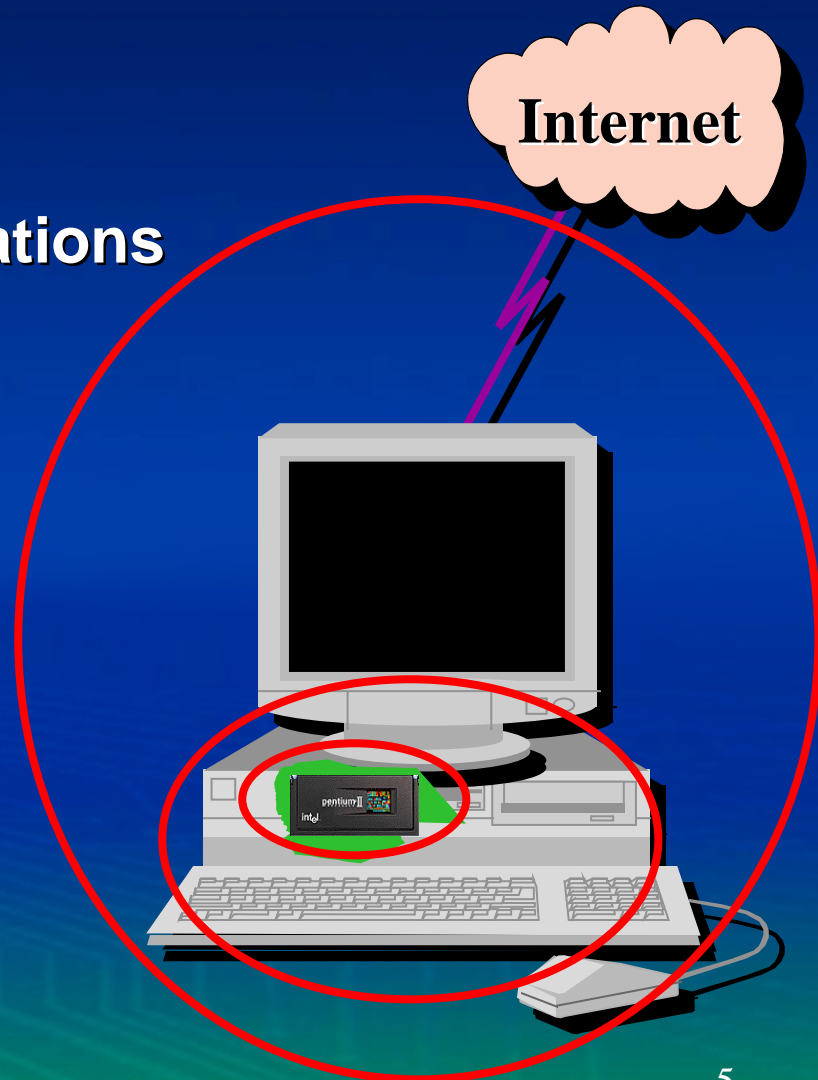
- Malicious Code / Virus
- Strong User Identification & Access Controls
- Extending network to remote employees, customers and suppliers
- Theft of Company Data
- Protecting information on the network

SOURCES:

- InfoTek Research Report 10/98
- Information Security Magazine - Security Survey 7/99
- CIS/FBI Security Report 1999

What Do We Need to Defend Against?

- **Hacker over the network**
 - Threat to secure communications
 - Spoofing, replay, denial of service
- **Malicious code**
 - Threat to local secrets
 - Viruses, Trojan horses
- **Illegal copying and theft**
 - Threat when “bits have value”

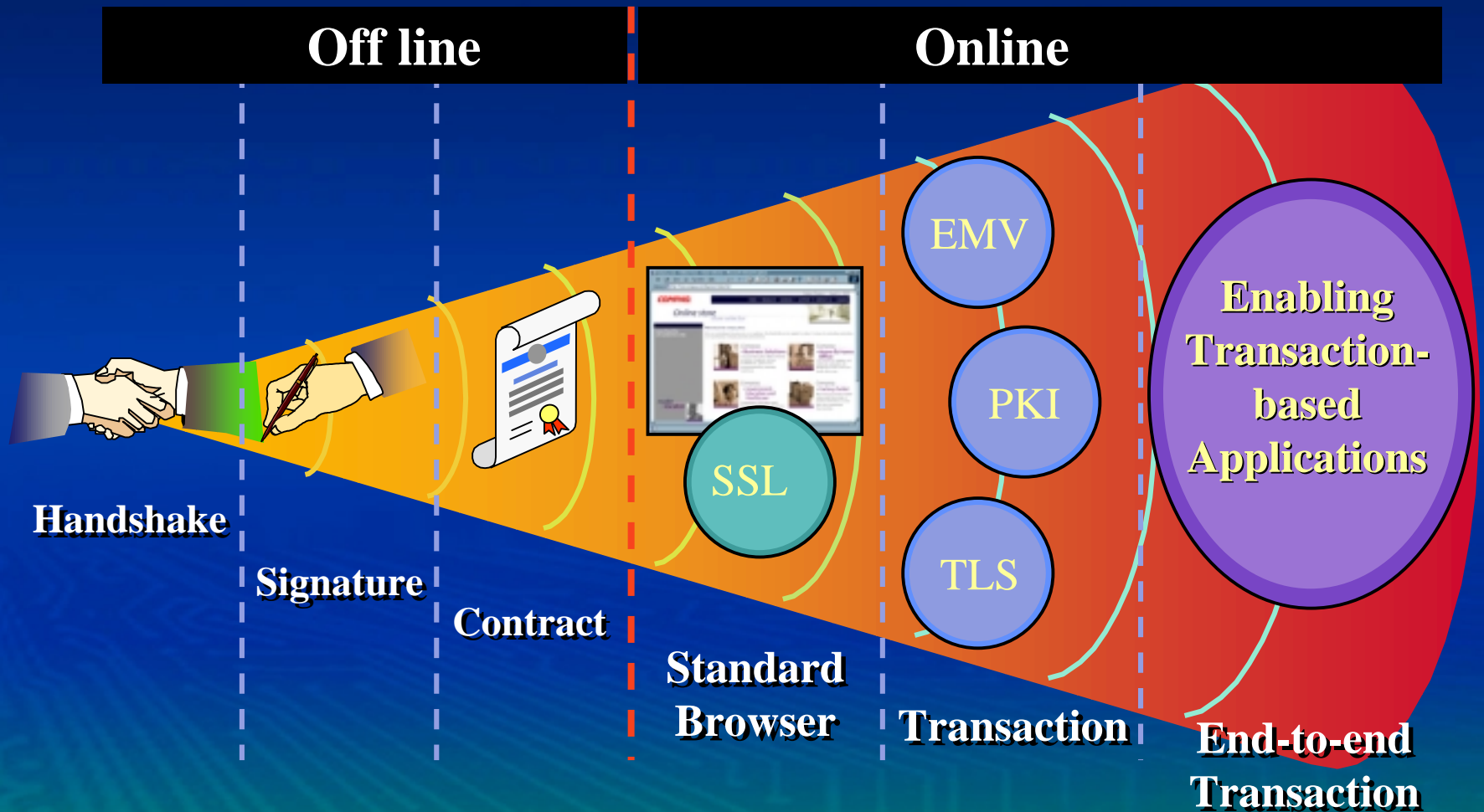


“Better Security” is a Challenge to Explain

- Internet commerce is growing wildly
- Many on-line users feel safe today
- Most executives believe their companies have good security
- Technology, policy, and user behavior all impact security

***Security and Privacy* Required for Trust**

How We Establish Trust



Agenda

- What is “Trust”?
- Designing Security into the Computing Environment
- Privacy Considerations
- Policy Directions

General Security View Today

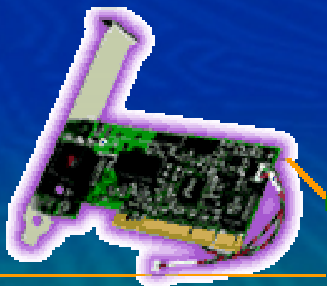
Enabling trust in e-Business

Security Alert



SSL: de facto protocol for web-based protected transactions

IPSec/VPN's: emerging standards for network security



PKI/Dig.Certs: 50% migrate in 2yrs as primary means to user authentication

Native OS support for Digital Certificates, smart cards, & IPSec



Windows*
2000

Industry Actions Needed

- **Set of baseline security features**
 - T CPA
- **Cost effective tokens and biometric capabilities**
 - PC/SC (and other organizations)
- **Privacy policies and practices**
 - OPA, ISTPA

Trusted Computing Platform Alliance

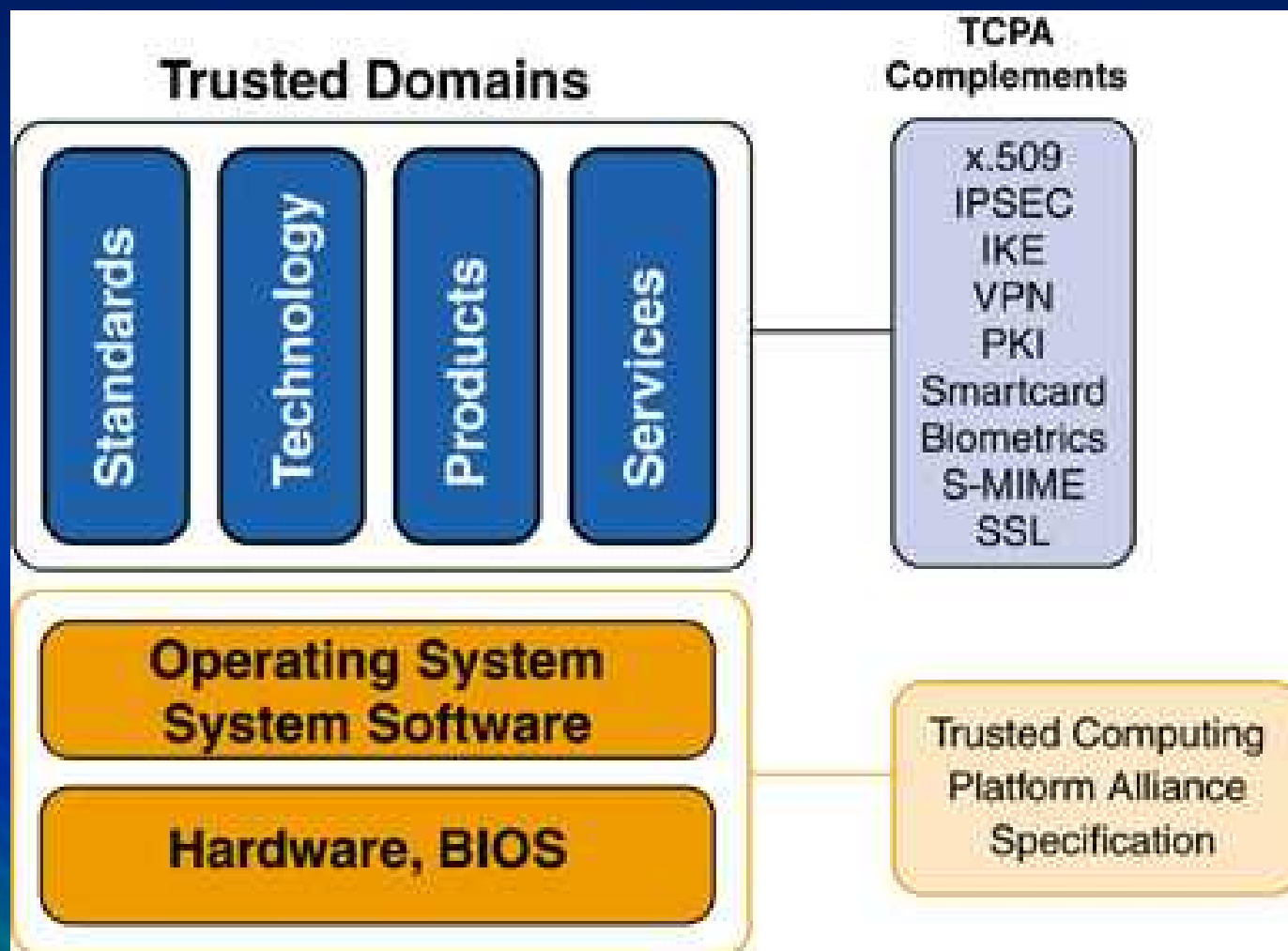


- **Objectives**

- Define scope of the problem and solution
- Develop and release a specification
- Encourage wide industry support and adoption of the solution
 - Must be exportable, ubiquitous over time
- Ensure owner control of privacy

Support and Grow e-Business

TCPA Specification Scope

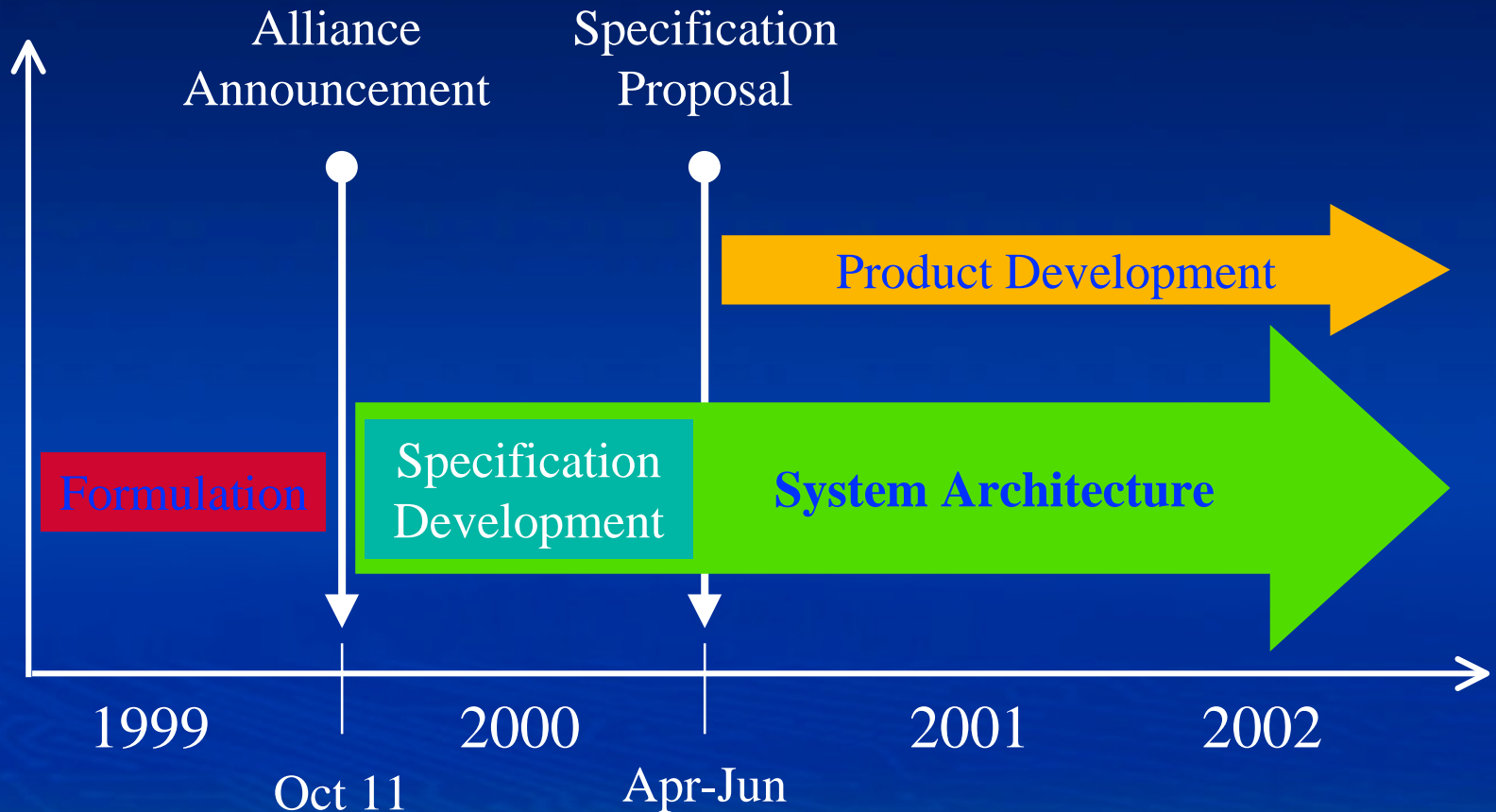


TCPA Specification Targets

- Security features proposed in V1.0
 - Protected storage of confidential information
 - Key Generation
 - Platform Authentication
 - Electronic signing of data
 - Hashing of data
 - Random number generation
 - Integrity metrics / challenge

Hardware + Software > Software Only

TCPA Timeline

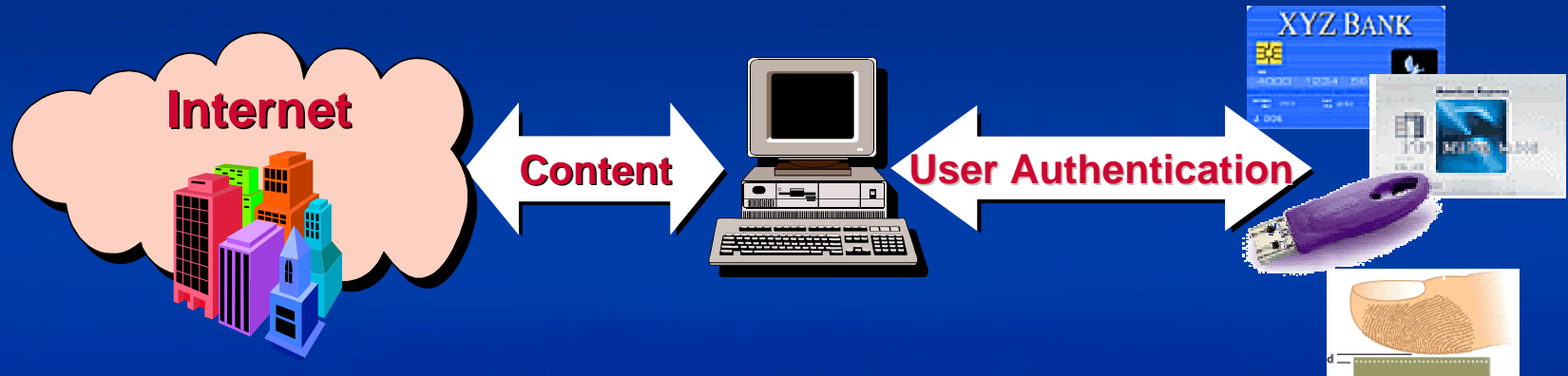


Currently at 80+ Members and Growing

**All dates provided are for planning purposes only and are subject to change

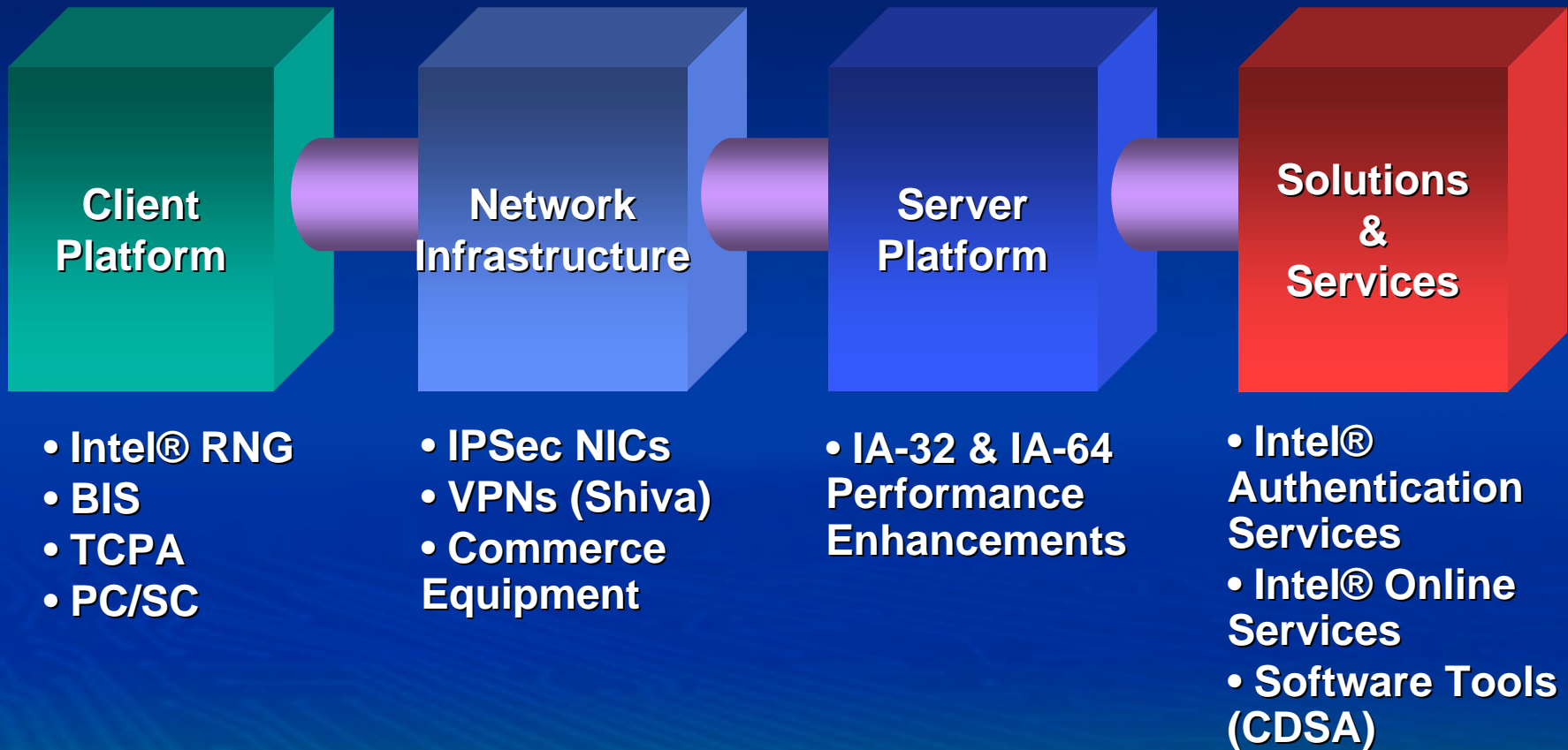
Smart Cards, Tokens, and Biometrics

- PC-complementary technologies
 - For Authentication, User ID, Access Control, Credential Storage



- Working to simplify integration into PC
 - TCPA, PC/SC Workgroup, BioAPI, Smart Card Forum
- Broad deployment requires:
 - Lower cost infrastructure
 - Compelling PC-based applications

Security is Core to Intel's Internet Building Blocks



Building Block Enablers *Clients & Servers*

Authentication/Confidentiality

*IPSec
Intel® Random Number
Generator
Biometrics
Smart Cards /Tokens*

Firmware Controls

*Boot Integrity Services
Passwords
DriveLock*
QuickLock*/QuickBlank**

Application Enabling

*Security Middleware:
CDSA*

Physical Controls

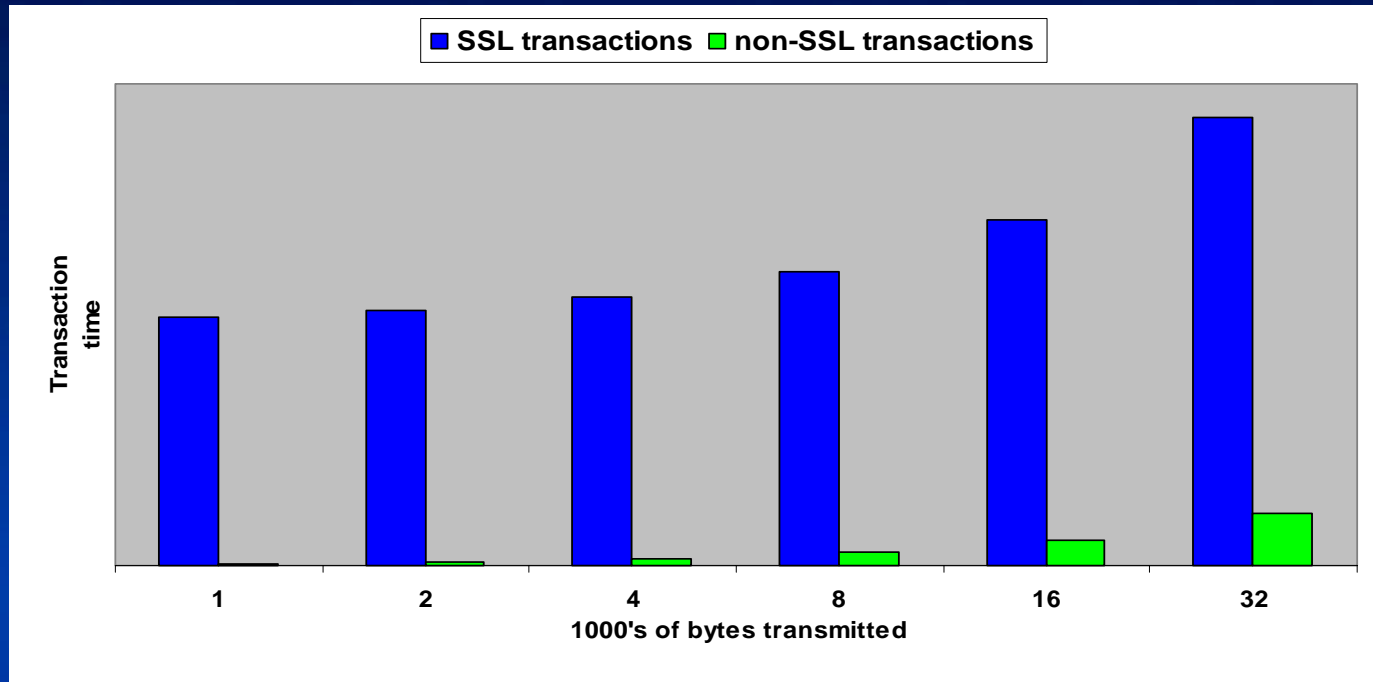
*Hood and cable locks
Smart cover lock
Security screws*

Remote Management

Alert on LAN
Chassis intrusion
Missing processor
Presence Heartbeat*



SSL Puts a Big Load on Servers



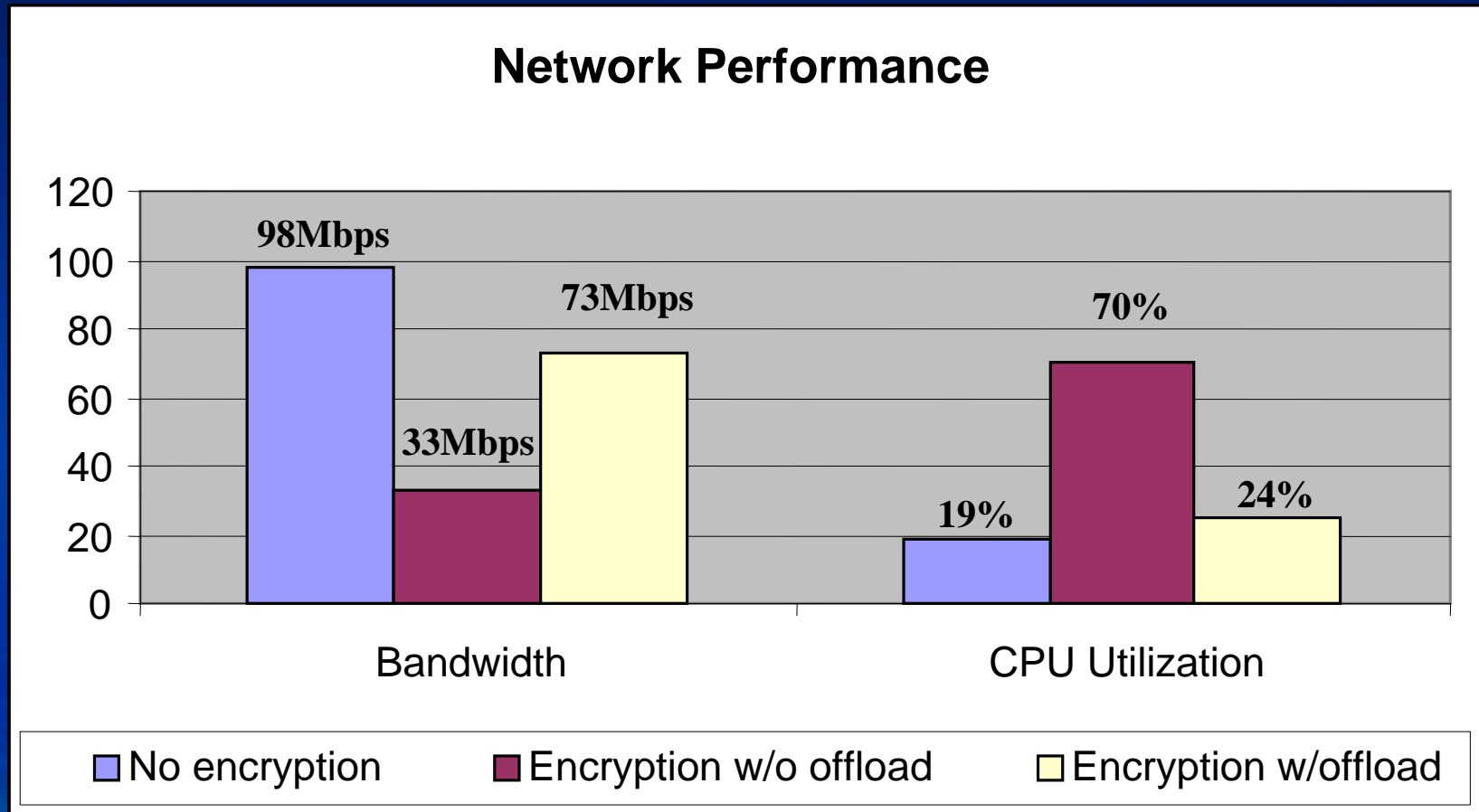
- Intel is developing faster processors with optimizations for security
- Intel® architecture-based servers have flexibility and scalability for demanding security applications

Intel's Security-enabled NICs

- Just launched this week
- Uses innovative encryption co-processor
- Supports Windows2000* right of the box
 - Drivers available for other OSs
- Accelerates IPSec encryption
 - Offloads to co-processor
 - Offloading encryption function speeds network performance

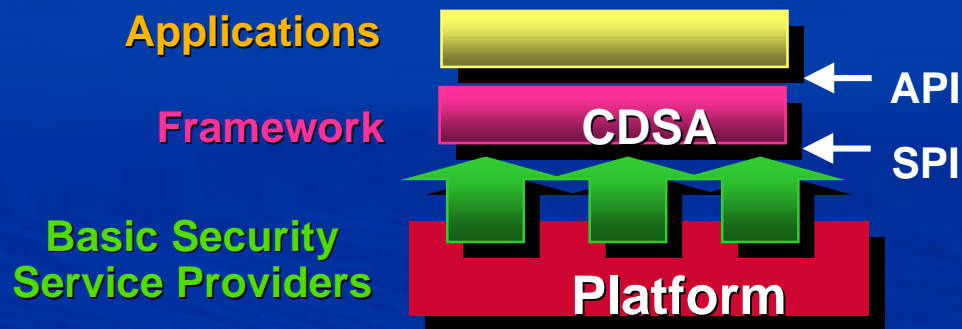


IPSec Performance



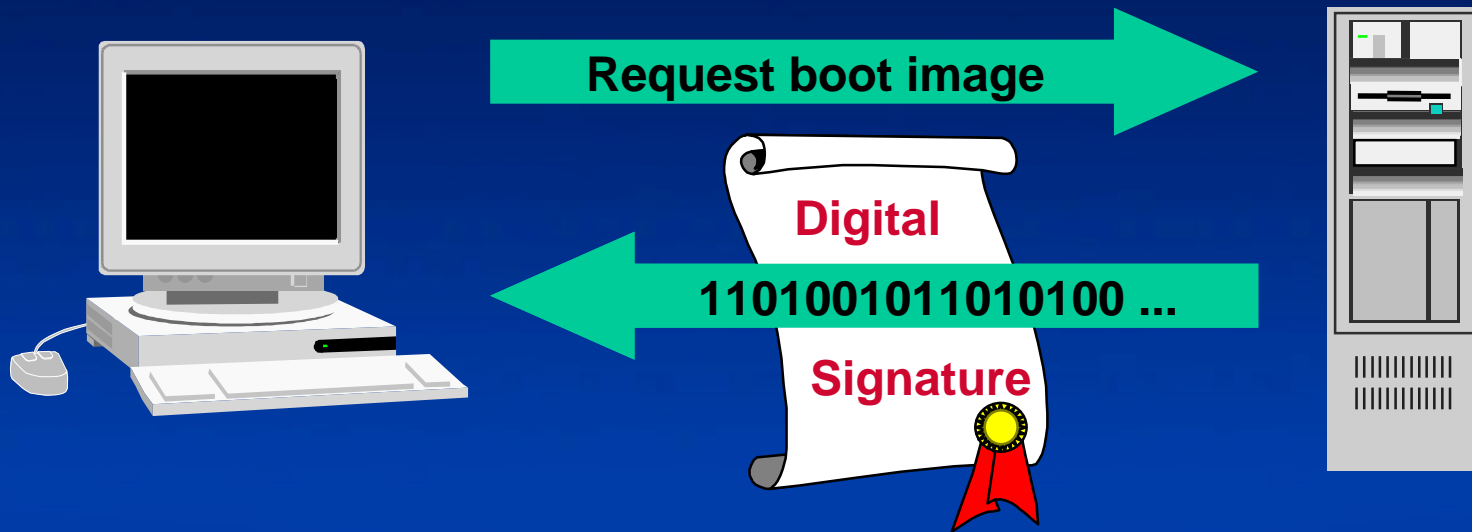
Common Data Security Architecture

- Open, interoperable, cross platform security infrastructure
- Over 5 years of R&D and industry review
- Version 2 Release 3.0 will ship in March



**Peer-reviewed, Robust, and
Ready for Broad Adoption**

Wired for Management: Boot Integrity Services (BIS)



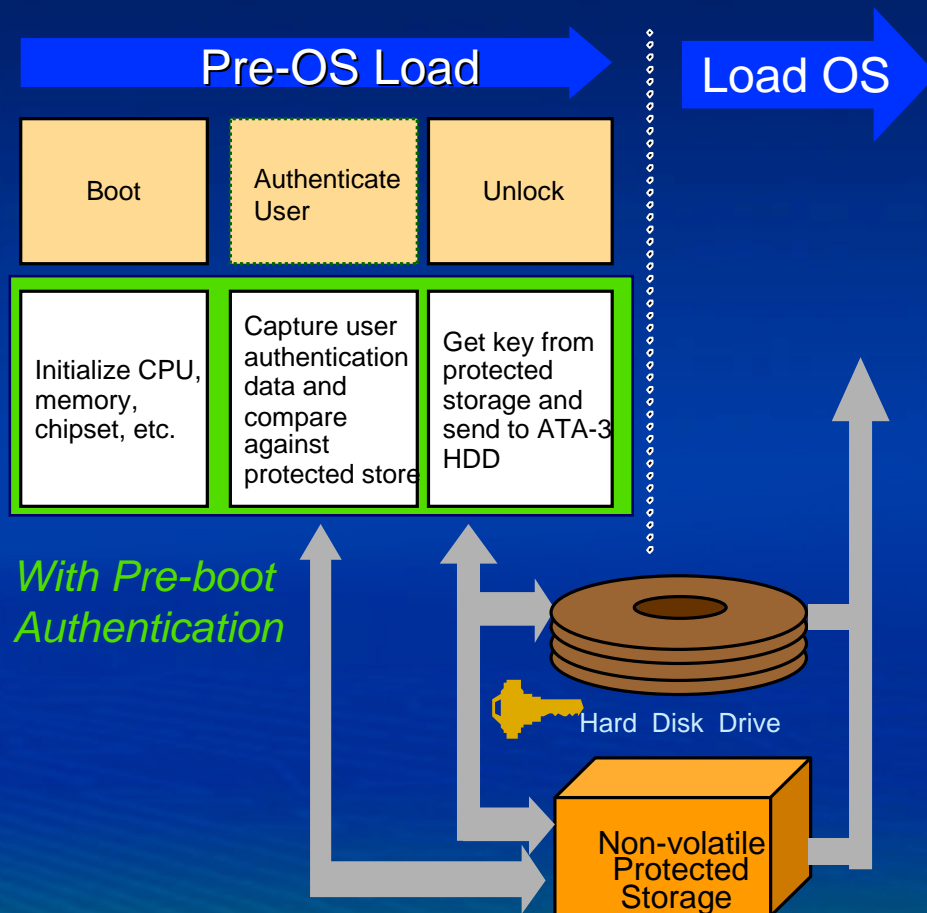
Boot image authentication

- Digital signature (public key) pre-stored in NV memory
- Downloaded program is accompanied by a digital signature (private key)
- BIS in the client performs verification

Increased Trust for Initial Software Download

Pre-boot Authentication

- Architecture and services to strengthen user authentication during boot-up
 - Supports multi-factor authentication
 - Creates a deterrent to notebook theft
 - Bus, token, and BIOS independent



Agenda

- What is “Trust”?
- Designing Security into the Computing Environment
- Privacy Considerations
- Policy Directions

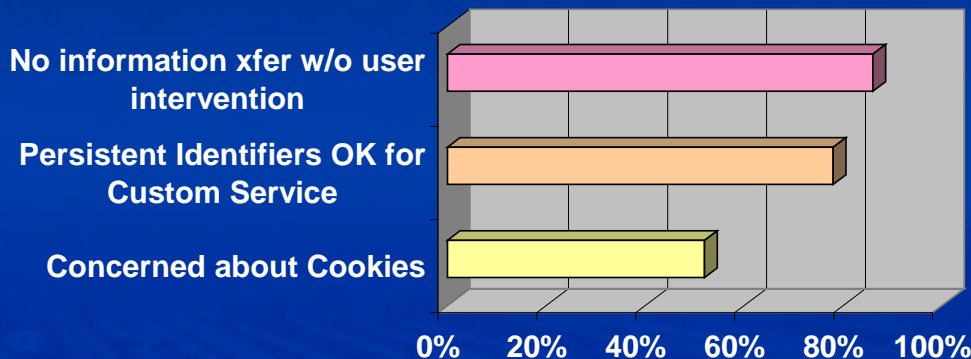
Privacy Was Top of Mind in '99

- And we helped...
- Privacy got the attention of various organizations
 - Government
 - Advocacy Groups
 - Media
 - Businesses

Privacy on the 'Net Remains a Concern

Privacy Data

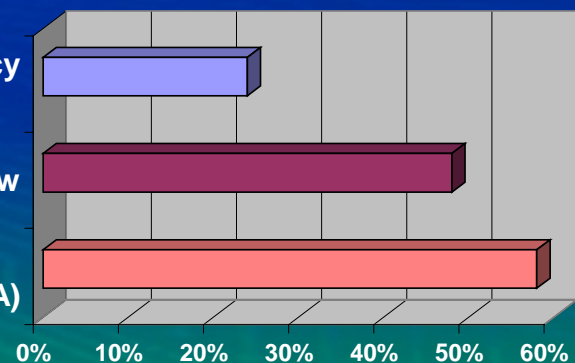
- Choose your source
- Conclusion's the same



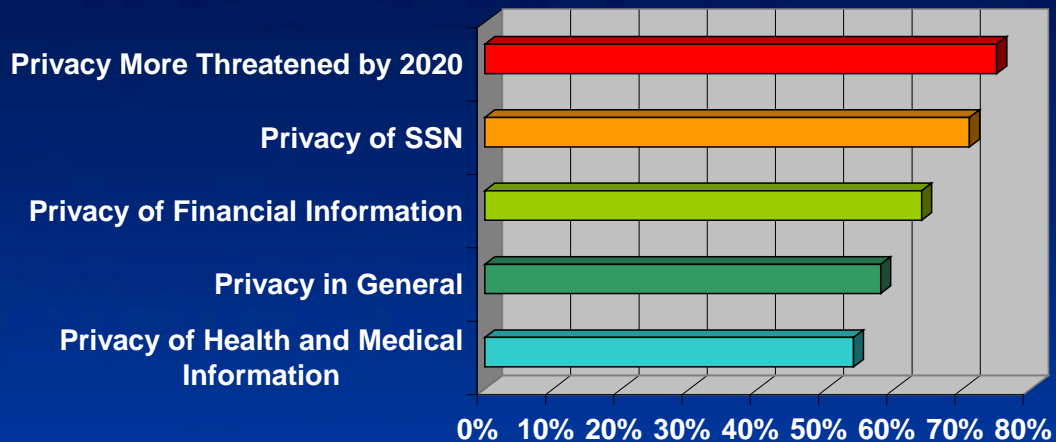
Provide info if privacy policy posted

Provide info if protected by Law

Provide info if privacy policy posted & seal (e.g. BBB or AAA)



Consumer Attitudes on Privacy



Source: Consumers and the 21st Century
Conducted for: National Consumers League
Louis Harris and Associates, 1999

Industry Action on Privacy

- Industry Working Groups



- Seal Programs



- Online Advertising Programs



Europe and Privacy

- **Recent Survey by Jupiter Communications:**
 - About 75% of EU sites collect data
 - Only 10% of EU sites have Privacy Policy linked to home page
 - 89% of EU sites not confident of compliance with EU directive
 - EU consumers willing to trade data for benefits
 - Security and Trust still barriers to buying online

Consumer communication and education is good business worldwide

Intel Privacy Principles

The screenshot shows a web browser window displaying the Intel Privacy Principles page. The browser's address bar shows the URL 'http://www.intel.com/privacy/'. The page has a blue header with the Intel logo and navigation links: 'intel.com home', 'product info', 'search', 'contact us', and 'support'. A left sidebar contains links for 'legal information home', 'trademarks and brands', and 'visit other intel sites'. The main content area is titled 'Intel's Privacy Principles' and includes sections on 'Consumer Choice', 'Informed Consent', 'Government and Private Actions', and a concluding statement about innovation and regulations.

intel.com home product info search contact us support intel.

legal information home

trademarks and brands

- [Usage Guidelines](#)
- [General Information](#)
- [Trademark Symbols](#)
- [Approved Names](#)
- [Third Party Use of Intel Code Names](#)
- [Contact Info](#)

visit other intel sites

- [Personal Technology](#)
- [Intel® e-Business Center](#)
- [Developer](#)
- [Channel](#)
- [Support](#)

Intel's Privacy Principles

Intel is committed to user privacy in our products and services.

To this end, Intel supports the following principles:

Consumer Choice

We believe the user is the one to best determine:

- When — and under what conditions — to provide "personally identifiable information"
- When to remain anonymous.

Informed Consent

If personally identifiable information is collected, we believe the user has the right to:

- Know when a website is collecting personal information
- Know what personal information is collected, and the purpose of collection
- Receive explicit notification before any personal information is collected
- Expect that personal information will not be provided to any third party without the user's permission
- Expect reasonable steps to be taken to protect personal information from unauthorized use
- Review the accuracy of personal information and update it

Government and Private Actions

We believe a market environment, supported by good consumer information and industry self-regulation, provides the most efficient way to support user privacy needs.

Independent "privacy seal organizations," such as TRUSTe and BBBOnline provide the customer with an additional level of assurance and we urge web sites to register with one or more such organizations. We also believe that these or comparable programs should be implemented worldwide.

Therefore, we have taken the following steps:

- Intel has registered with TRUSTe and displays the TRUSTe seal on our web site's privacy policy. Intel is also a corporate sponsor of TRUSTe.
- Effective September 1, 1999, Intel will only purchase advertising space on web sites posting a comprehensive privacy policy that meets the guidelines of the Online Privacy Alliance ("OPA")
- Cooperative advertising licensees are being urged to follow a similar policy, which will become a U.S. program requirement as of January 1, 2000. Similar requirements will be implemented in other countries as local guidelines are established by similar regional organizations.

If laws and regulations are created, we believe they should support innovation and a technology-neutral framework to maximize the choices available to users, product suppliers and service providers. Intel will comply with all applicable laws where we conduct business.

Agenda

- What is “Trust”?
- Designing Security into the Computing Environment
- Privacy Considerations
- Policy Directions

Policy Considerations

- **Government**
 - Legislation
 - Export Controls
 - Technology



We must make [our critical systems] more secure so that America can be more secure.
- Bill Clinton, Jan 6, 2000

- **Corporate**
- **User Awareness / Comfort**
- **Privacy**

Legislation

- Self-regulation and market forces provide greatest flexibility
- Specification of capabilities offers much more flexibility than specification of technologies
- Technology limitations need to be comprehended when developing legal accountability of digital signatures

Technology Changes Continually

Summary

- Intel is designing security into Client, Server, and Network products as well as Services
- The industry is banding together and creating specifications for interoperability
- Privacy remains a user concern that must be considered in all products
- Export policies are improving - but security concerns are growing around the world

“It takes an industry to build a trusted, connected world”